MALWARE PARA DISPOSITIVOS MÓVILES (ANDROID)

Daniela Muena Bustos

Universidad Tecnológica de Chile INACAP
Ingeniería en Informática, Chillán.

daniela.muena@inacapmail.cl

ABSTRACT

This paper aims to show research papers in Android malware detection and also mention safety measures to prevent or detect malware on your mobile device.

Palabras claves

Malware, troyano, ransomware, botnet, seguridad, medidas de seguridad, dispositivos móviles, Smartphone.

1. INTRODUCCIÓN

En la actualidad no sólo los computadores de escritorio y notebook son propensos a ataques de seguridad, sino que también los dispositivos móviles que tienen acceso a internet. Figura Nº 1,

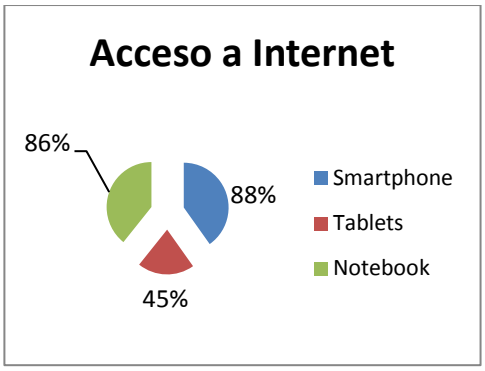


Figura Nº 1: "Acceso a Internet"

Hoy en día, los dispositivos móviles como el Smartphone son indispensables para las actividades cotidianas que se realizan en nuestras vidas.

Los teléfonos inteligentes o Smartphone poseen toda nuestra información, ya sea contactos, fotografías, videos, datos bancarios, correos electrónicos, datos de las redes sociales. Si le ocurre algo a nuestro Smartphone prácticamente ya no estamos conectados con el mundo que nos rodea.

Figura Nº 2 muestra un estudio de IAB Spain demuestra que del año 2013 un 80% tenía Smartphone y al año 2014 ha aumentado a un 87%. Los rangos de edades que más aumentaron en poseer Smartphone son de 26-45 años y el 46-55 años del 2013 al 2014 ha aumentado de 10 a 13 respectivamente [1].

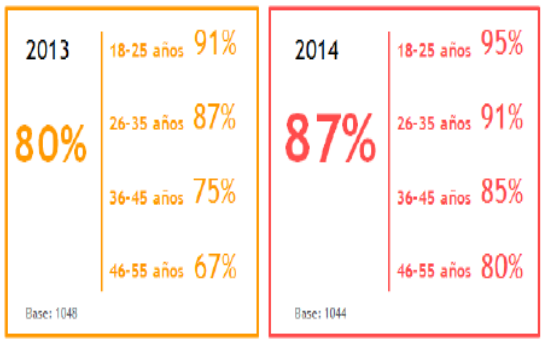


Figura Nº 2: "Rango de edad que tienen Smartphone"

Figura Nº 3 muestra el estudio de AVG-Comparatives el 85,4% de los encuestados tiene un móvil. De estos, el 70,1% utiliza S.O Android, el segundo lugar lo ocupa iOS de Apple con el 14,9%, seguido de Windows Mobile con el 7,8% [2]. Android es el sistema operativo más popular

entre los usuarios de Smartphone pero también su popularidad los hace un blanco atractivo para los autores de malware.

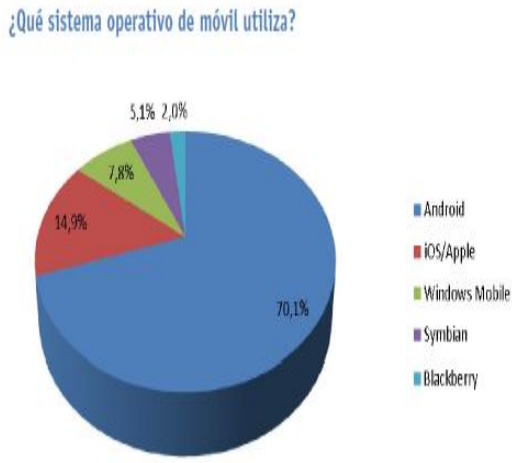


Figura Nº 3: "Porcentajes de cada SO móvil"

El trabajo se compone de la siguiente manera. En el número 2, se explicará la metodología de investigación y se mencionarán las preguntas de investigación. Número 3, la estrategia que se usa en la investigación. Número 4, Cual es el propósito del trabajo de investigación. Número 5, se explicará que es Android, una breve historia de sus orígenes y también su arquitectura. Número 6, se explicara la historia del malware en Android hasta el año 2013. Número 7, se mencionarán distintos tipos de malware que afectan a la plataforma Android. Número 8, medios de propagación de malware, se mencionarán algunos medios que son importantes. Número 9, se mencionarán algunas propuestas hechas por investigadores extranjeros sobre posibles técnicas para la detección de malware. Número 10, se darán medidas de seguridad que los usuarios podrían realizar para protegerse mejor de los malware, teniendo en cuenta que la responsabilidad de cuidar de nuestros dispositivos es de cada usuario y el número 10 se concluye el documento con lo más relevante.

2. Metodología de la Investigación

En el trabajo se ha realizado una revisión de documentos y sitios web sobre el malware móvil en el sistema operativo Android, con el objetivo de presentar los medios de propagación del malware a Android y a su vez también mostrar algunas técnicas de detección de malware. A continuación las preguntas de investigación:

P1: ¿Qué tipo de malware afecta al sistema operativo Android?

P2: ¿Cuáles son los medios de propagación del malware a los dispositivos?

P3: ¿Existen técnicas de detección de malware?

P4: ¿Por qué es atractivo para los desarrolladores de malware la plataforma Android?

P5: ¿Cuáles podrían ser medidas de seguridad o de prevención de malware que los usuarios podrían implementar?

3. Proceso de la revisión

La estrategia que se utiliza es la revisión de documentos validados internacionalmente y sitios web de empresas reconocidas y otros sitios web de más bajo nivel. La antigüedad de los artículos es del año 2012 hasta el año 2014. 7 documentos son publicaciones pertenecientes al IEEE Xplore. Otros son documentos de empresas como McAfee, ESET, IAB Spain, Kaspersky Lab, Av-Comparatives.

El propósito

El problema planteado son las amenazas que tiene la plataforma Android desde sus inicios, es decir, estas amenazas son el malware, todo archivo con contenido de carácter malicioso y posibles técnicas de detección de malware.

4. Android

4.1 ¿Qué es Android?

Android es un sistema operativo y plataforma software, es el sistema operativo de Google para teléfonos inteligentes. Basado en Linux, es un sistema gratuito y multiplataforma. Por multiplataforma se entiende que el SO puede ser usado en distintas plataformas (plataforma es una combinación de hardware y software usada para ejecutar aplicaciones) y por gratuito es por ir instalado gratis en el dispositivo [10]. El logo del sistema operativo Android es Andy, como muestra la Figura Nº 4.

Figura Nº 4: "Andy, el robot de Android"

4.2 Historia de Android.

En octubre del 2003, Andy Rubin, Rich Miner, Nick Sears y Chris White daban forma a Android Inc. El éxito de Android es el 5 de noviembre de 2007, ese día se fundaba la OHA (Open Handset Alliance), una alianza comercial de 35 componentes iniciales liderada por Google, que contaba con fabricantes de terminales móviles, operadores de telecomunicaciones, fabricantes de chips y desarrolladores de software. Google es quien ha publicado la mayor parte del código fuente del sistema operativo, gracias al software Apache, que es una fundación que da soporte a proyectos software de código abierto.

En Octubre de 2008, es cuando se ve por primera vez funcionando Android en un HTC Dream como lo muestra la Figura Nº 5. También el éxito de Android es el Android Market, el almacén de aplicaciones más popular [10].

Figura Nº 5: "HTC Dream con SO Android"

4.3 Arquitectura de Android.

La arquitectura de Android se compone de cinco capas como lo muestra la Figura Nº 6.

- La capa superior es la capa de aplicación, que entra en contacto con el usuario que contiene todas las aplicaciones que corren sobre el sistema [7] [11].

- La capa marco de aplicación, provee diferentes servicios para las aplicaciones, la existencia de la capa se debe a la necesidad de controlar el acceso a la información. Esta capa facilita sustancialmente la tarea a los programadores de aplicaciones [7].

- La capa de bibliotecas, está escrito en el lenguaje C y se puede acceder rápidamente a varias funciones tales como diseño de página, base de datos, etc [11].

- El tiempo de ejecución de Android, consta de bibliotecas principales de OS y Dalvik máquina virtual. La maquina virtual Dalvik, funciona en múltiples máquinas virtuales a través de una mayor estabilidad y menor cantidad de uso de memoria, ya que se asigna a cada proceso [11]. Es decir, cada aplicación se ejecuta como "un usuario" corriendo

sobre su propio Dalvik Virtual Machine [7].

- La capa inferior Kernel Linux, incluye controladores para la gestión del sistema operativo, directamente la gestión de hardware o de realizar tareas muy relacionadas [11]. Este kernel es multi-usuario, esto quiere decir, que pueden estar corriendo aplicaciones de diferentes usuarios sin que "interfieran entre sí" [7].

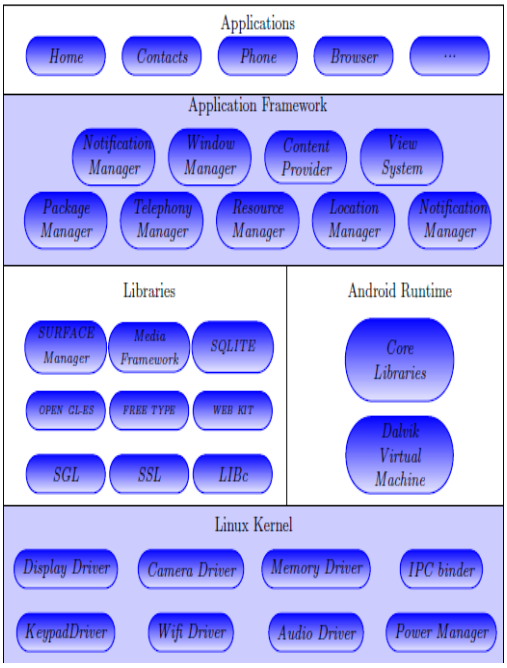


Figura Nº 6: "Arquitectura de Android"

5. Historia de malware móvil Android

El malware ya no es solamente en los computadores sino que también ha llegado a los teléfonos inteligentes y la principal víctima es el sistema operativo Android por su popularidad entre los usuarios, así como sus vulnerabilidades y vías de infección, como por ejemplo, que el mercado oficial de Android no analiza las aplicaciones que se incluyen en el mercado.

El concepto de Malware viene de las fusiones de las palabras en inglés "Malicious + software", que sería software malicioso. Es cualquier software que sin el conocimiento del usuario realiza acciones consideradas poco éticas [7].

A continuación, se mencionarán algunos malware móvil para Android, cronológicamente, los que más dejaron historia:

- **FakePlayer:** En Agosto de 2010 [3] [4], Dennis Maslennikov de Kaspersky descubrió el 1º troyano SMS para Android. Aparece en una aplicación de reproductor multimedia con un icono falso Windows Media Player (Figura Nº 7), esta aplicación envía SMS a servicios Premium sin el consentimiento del usuario.

Figura Nº 7: "Icono de Windows Media Player falsa"

- **GPS Spy:** En Agosto del 2010 Symantec descubrió el primer GPS software malicioso. Este malware se encontraba disfrazado en un juego de serpiente. Tenía la capacidad de reunir y enviar coordenadas GPS a un servidor remoto [3].

- **Geinimi:** A finales del 2010, se descubrió un troyano que afecta a los dispositivos Android. Es el primer software malicioso que muestra características de botnets tradicionales [3]. Geinimi demostró la posibilidad de "infectar" aplicaciones legitimas con código malicioso. Estas aplicaciones legítimas como Monkey Jump 2, Presidente vs Aliens, City Defense y Baseball Superstars 2010 [4].

- **Pjapps:** Es otro ejemplo de una aplicación que contiene un troyano y que muestra características de un bot tradicional. De mercado de

terceros aparece este malware. Permite que se abra una puerta trasera (backdoor) en el dispositivo y recibe comandos de un servidor remoto [3].

- **DroidDream:** Apareció en marzo del 2011 [5], infectó a más de 50 aplicaciones en el mercado oficial de Android, con la aparición de este malware aparece una nueva era de malware para Android. Robo de datos, exploits de root y funcionalidad de botnets. El objetivo era establecer una botnet [3].

- **ZitMo:** Apareció por primera vez en dispositivos Android en Julio de 2011. Infecta aplicaciones legítimas y trabaja junto al troyano bancario Zeus para robar información bancaria [3].

- **NickiBot:** Se descubrió a finales de 2011, utiliza mensajes SMS para dirigir y controlar. Se encontró solo en mercados no oficiales de Android.

- **FakeInst:** Apareció en el año 2012, es un troyano SMS que se disfrazo como aplicaciones más populares, lo que hace es enviar mensajes SMS a números de tarifación adicional [6].

- **SMSZombie:** Aparece en el año 2012, en los mercados de terceros en China y explota el sistema de pago en línea de China Mobile, al estar instalado en el dispositivo obtiene permisos administrativos, lo que provoca que sea difícil eliminarlos [6].

- **NotCompatible:** Aparece en el año 2012, fue descubierto por Lookout Mobile Security, es el primer malware en usar sitios web como un método de propagación, infecta Smartphone cuando visita a un sitio web en específico [6].

- **Androi.Bmaster:** Aparece en el año 2012, es una red de bot móviles, incluido con aplicaciones legítimas y generó un ingreso diario entre 10.000 y 30.000 dólares [6].

- **LuckyCat:** Aparece en el año 2012, dirigido a industrias aeroespaciales y de energía en Japón, causa una puerta trasera (backdoor) que se abre en el dispositivo infectado [6].

- **FakeDefender:** Aparece en año 2013, el primer ransomware para Android, se descargaba como si fuera un antivirus pero bloqueaba el dispositivo y además pide un rescate para desbloquearlo [8].

6. Tipos de Malware

Existen diversos tipos de malware para el sistema operativo Android, las causas de la propagación de malware sean las distintas formas de distribuir las aplicaciones, como se muestra en la Figura Nº 8, los usuarios de Android no sólo pueden descargar aplicaciones del mercado oficial de Android, sino que también de sitios alternativos y página web de desarrolladores [7]. De su mercado oficial tampoco es tan seguro, ya que no analizan las aplicaciones que suben los desarrolladores al mercado, siendo quizás hasta aplicaciones con fines maliciosos.

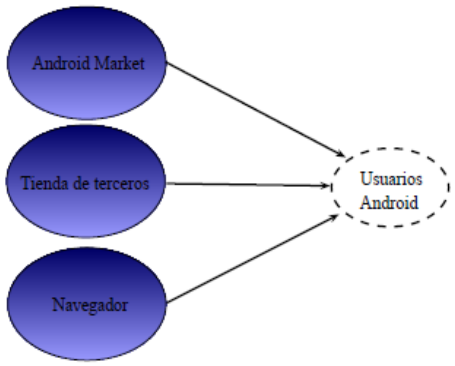


Figura Nº 8: “Distribución de aplicación en el SO Android”

A continuación se mencionarán tipos de malware que se ha descubierto afectan al sistema operativo Android:

6.1 Troyano SMS

Este malware sin el consentimiento del usuario, lo que hace es enviar mensajes de texto SMS a números Premium, es decir, a números que al enviar mensajes cobran mucho más que al enviar mensajes a números normales [7].

6.2 Worms

O también conocidos como gusanos, son aplicaciones que pueden auto reproducirse hasta llegar a saturar algún recurso del sistema. Su fin es solamente destruir el sistema no para obtener beneficios del dispositivo [7].

6.3 Spyware.

Software espía, aplicación no autorizada que captura datos privados y es capaz de trasmitirlos a algún receptor. Su primera función principal es recoger información sea del sistema o de alguna aplicación, segunda función es transmitir esta información y la tercera es seguir oculto lo más que se pueda [7].

6.4 Botnet.

El botnet no solamente infecta a PC sino que también ya ha aparecido para los Smartphone. Una botnet se define cualquier grupo de PC infectados y controlados por un atacante de forma remota. Son llamados “bots” o “zombie”, crea un botnet a través de un malware que infecta a una gran cantidad de máquinas. Es decir, es una gran red de ordenadores o dispositivos móviles infectados con una variedad de malware [14]

6.5 Ransomware.

Es un software malicioso que bloquea el PC desde una ubicación remota y encriptar los datos almacenados y archivos y para desbloquearlo pide una suma de dinero, para el rescate. Antiguamente ransomware se utilizaba para los PC pero ya ha llegado también a los dispositivos móviles como el Smartphone [15].

7. Medios de propagación de malware

Aquí se explican algunos medios de propagación de malware:

1. **MMS/SMS:** Pueden extenderse a otros dispositivos móviles adjuntando una copia de si mismos en mensajes de MMS/SMS que se envía desde el dispositivo infectado. Envía mensajes a todos los números de contacto que tenga el móvil o genera combinaciones de números de teléfono específicos de un operador o región [10].

2. **Bluetooth:** Depende de la proximidad física del atacante a la víctima. El teléfono debe estar en modo de detección [10].

3. **Sitios Web:** En la mayoría de los casos, son paginas legítimas que pertenecen a empresas de diversos rubros y que por causa de alguna vulnerabilidad, protección insufieciente o configuración inadecuada, son modificadas por el atacante que ha logrado obtener acceso al servidor [12].

8. Propuestas de seguridad para Android

En esta sección del trabajo se mostrarán algunas propuestas hechas por investigadores para detectar malware:

a) MDoctor: Un pronóstico de aplicaciones móviles de Malware por Eemil Lagerspetz, Hien Thi Thu Truong, Sasu Tarkoma, N. Asokan [16].

Esta investigación es una aplicación de pronóstico móvil de malware basado en datos crowdsourced. MDoctor puede determinar la salud del dispositivo basado en cuatro indicadores: confianza del mercado de aplicaciones, confianza clave del desarrollador, correlación con el malware y combinación con malware conocido (de su conjunto de datos de malware). Como se muestra en la Figura Nº 9, la aplicación muestra secciones de color amarillo o rojo para aplicaciones sospechosas de infección. En la parte (A) se muestra el estado inicial de la aplicación. (B), (C) y (D) muestran a la aplicación, al seleccionar un trozo se muestra la información, si se detecta o no malware.

Este trabajo de investigación no sólo pronostica la infección de malware, sino que también puede alertar de un posible riesgo de infección a futuro.

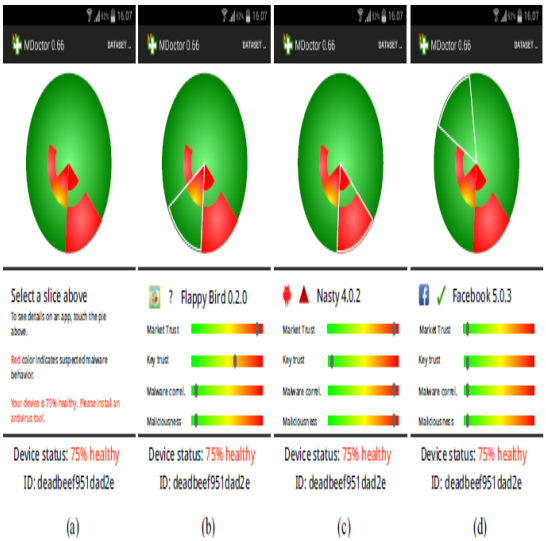


Figura Nº 9: "Muestra el estado de las aplicaciones del cliente de Android"

b) Seguridad de los teléfonos móviles: Los métodos de prevención para la propagación de malware por Mohamed Ghallali y Bouabid El Ouahidi [9].

Ellos propusieron una solución basada en los servicios ofrecidos por los proveedores de telecomunicaciones que deben garantizar más recursos para sus suscriptores, que un solo dispositivo móvil puede ofrecer, tales como servicios para detectar y eliminar virus de correo electrónico y virus web.

Si estas soluciones son instaladas en la red local del proveedor como muestra la Figura Nº 10, se puede detener la difusión de cualquier programa malicioso a través de la red. Esta solución incluye una completa solución de seguridad (antivirus de Gateway, firewall, detección de intrusos, análisis

de vulnerabilidad y filtro de SMS/MMS Antispam) [9].

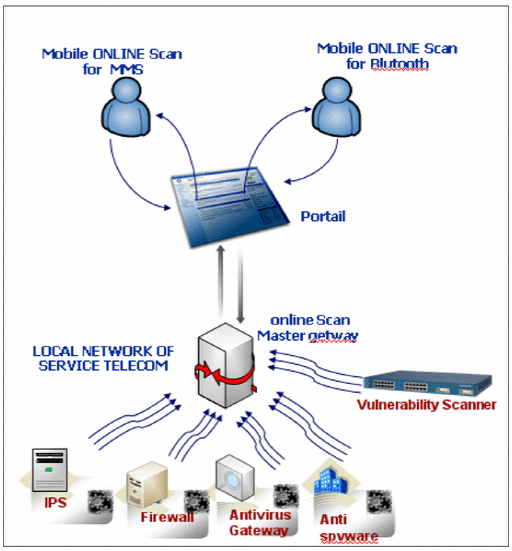


Figura Nº 10: "Servicios en línea del proveedor de telecomunicaciones se puede escanear/desinfectar los teléfonos móviles"

c) Análisis de Clustering Técnica en Android Malware Detection por Aiman A. Abu Samra, Kangbin Yim y Osama A. Ghanem [5].

Para este experimento se usaron 18.174 aplicaciones para Android, como muestra la Figura Nº 11, se utilizó dos categorías de aplicaciones Android: Negocios y Herramientas. La primera categoría tiene 4.612 muestras y el segundo tiene 13.535 muestras. Se calculó la precisión, recordar y F-medida y los resultados se muestran en la Figura Nº 12, con 0.71, 0.71 y 0.71, respectivamente. Los falsos positivos y falsos negativos tienen los mismos resultados 0.2897 [5].

Los resultados muestran una indicación positiva de utilizar esta metodología en automático de las categorías de las aplicaciones Android, mediante el uso de técnicas de agrupamiento y se utiliza para la detección de aplicaciones maliciosas de gran tienda de aplicaciones [5].

Application Categories	Number of samples
Business	4,612
Tools	13,535
Total	**18,174**

Figura Nº 11: "Número de muestras de aplicación de cada categoría de conjunto de datos de prueba"

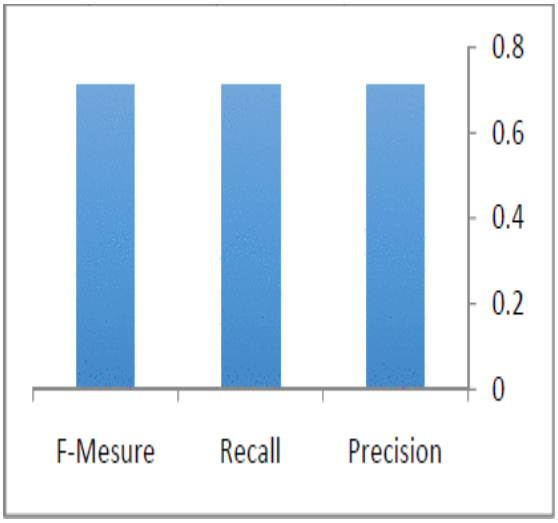
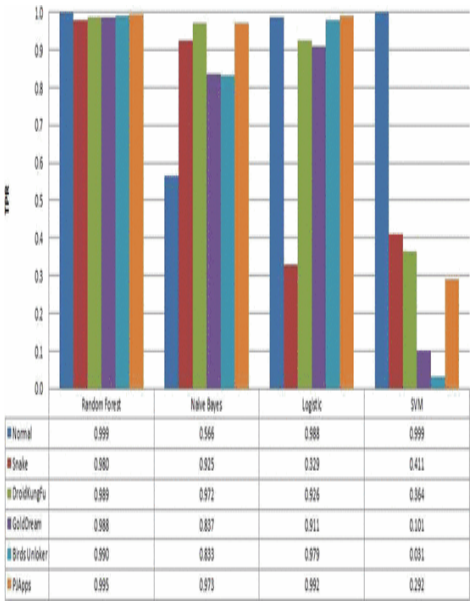


Figura Nº 12: "Precisión, Recordar y F-medir valores para experimentos"

d) Análisis de Android rendimiento de detección de malware utilizando clasificadores de aprendizaje automático por Hyo-Sik Ham y Mi-Jung Choi [11].

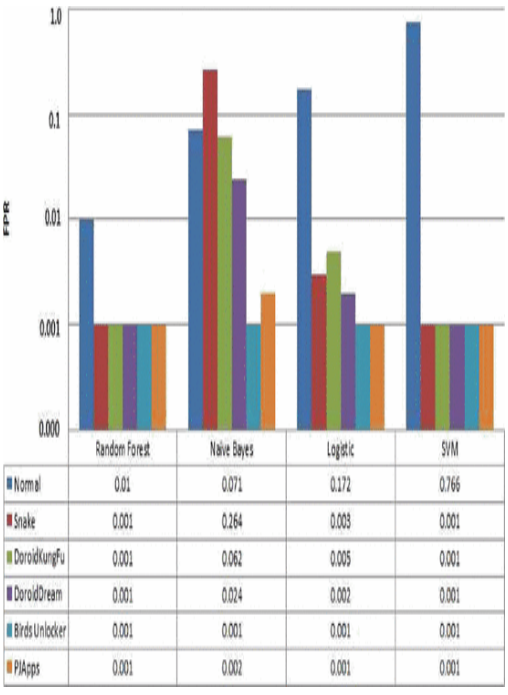
En esta investigación se llevó a cabo la evaluación del desempeño en cuatro tipos de clasificadores de aprendizaje automático para detectar con precisión malware. Los resultados experimentales mostraron que el clasificador

Random Forest tuvo un mejor rendimiento que los demás en TPR (verdadera tasa positiva), como muestra la Figura Nº 13 y FPR (tasa de falso positivo), como muestran la Figura Nº 14.



	Random Forest	Naive Bayes	Logistic	SVM
Normal	0.999	0.566	0.988	0.999
Snake	0.980	0.825	0.329	0.411
DroidKungFu	0.989	0.972	0.926	0.864
GoldDream	0.988	0.837	0.911	0.101
Birds Unlocker	0.990	0.833	0.979	0.031
PJApps	0.995	0.973	0.991	0.292

Figura Nº 13: "TPR (verdadera tasa positiva) de la máquina clasificadora de aprendizaje"



	Random Forest	Naive Bayes	Logistic	SVM
Normal	0.01	0.071	0.172	0.766
Snake	0.001	0.264	0.003	0.001
DoroidKungFu	0.001	0.062	0.005	0.001
DoroidDream	0.001	0.024	0.002	0.001
Birds Unlocker	0.001	0.001	0.001	0.001
PJApps	0.001	0.002	0.001	0.001

Figura Nº 14: "FPR (tasa de falso positivo) de la máquina clasificadora de aprendizaje"

9. Medidas de seguridad para los usuarios

A continuación se darán algunas medidas que los usuarios podrían utilizar para detectar o prevenir ataques de malware [6]:

- Instalar antivirus y aplicaciones de seguridad móvil. Según un informe de NORTON by Symantec [13], los usuarios tienen mayores conocimientos sobre seguridad en PC y menos conocimientos en los dispositivos móviles como muestra la Figura Nº 15. Además de mantener actualizadas los antivirus y aplicaciones, también se debe actualizar el sistema operativo del móvil.

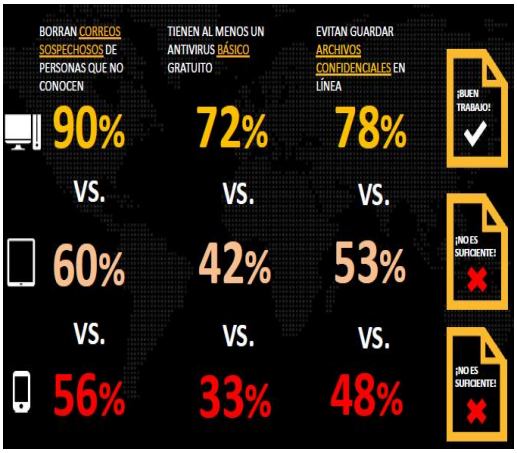


Figura Nº 15: "Conocimientos de usuarios"

- Por seguridad del dispositivo móvil nunca intentar arrancar de raíz para obtener privilegios de superusuario, al hacerlo le da ventajas al malware de poder usar el privilegio de superusuario y llegar a

dejar el dispositivo con mayores daños.

- Como se muestra en la Figura Nº 8, hay diferentes formas de descargar aplicaciones como en la tienda oficial de Android o tiendas de terceros o también de sitios web de los desarrolladores. Por supuesto, la responsabilidad es de cada usuario donde descargan aplicaciones, teniendo en cuenta que donde existe mayores probabilidades de encontrar malware son en los mercados de terceros.

- Mantener desactivado o apagado Bluetooth, Wi-Fi y/o NFC cuando no se están ocupando en el dispositivo y siempre que se ocupen intentar conectarse a redes seguras. Al igual por ejemplo en la noche apagar la red de datos, esto evitará que el malware se conecte con internet. Al igual que si no es necesario, mantener apagado GPS del Smartphone para prevenir la ubicación de donde se encuentra.

- Verificar las cuentas de factura del Smartphone, es decir, revisar si a gastado dinero de su teléfono, si es así, podría ser actividades maliciosas en su teléfono e investigar las posibles causas, como por ejemplo el envió de mensajes de SMS o llamadas telefónicas a números de tarificación adicional.

- Revisar los permisos cuando vaya a instalar alguna aplicación al teléfono. Esto quiere decir, que lea los permisos que se pide para instalar la aplicación y si son realmente necesarios para que la aplicación funcione. En caso que encuentre que podría ser maliciosa suspenda su instalación o no la instale.

- Conocer sus archivos almacenados en sus teléfonos, estar al tanto de todas sus aplicaciones y archivos que se encuentran almacenados con el fin de poder detectar si existen otros archivos que posiblemente sean maliciosos.

- Comprobar el consumo de la batería y el consumo de datos. El consumo de energía de la batería se podría monitorear con frecuencia para verificar si hay una disminución en la energía de la batería, si existe esta disminución es posible que sea algún contenido malicioso. El consumo de datos debería verificarlo semanal o mensualmente, para comprobar si en un periodo determinado hubo un pequeño consumo de datos, esto quizás podría ser algún malware en el móvil.

- Eliminar todas las aplicaciones y archivos

que ya no usan, además de eliminar archivos o aplicaciones que sean maliciosas y que hayan sido detectadas, para poder prevenir contenido malicioso que se haya alojado en otras aplicaciones o archivos.

10. Conclusión

Hoy en día, los ciberdelicuentes le tienen un gran “cariño” a los dispositivos móviles sobretodo del sistema operativo Android. Día con día ocurre más incremento de malware para los dispositivos y por ello se debe tener una mayor conciencia de que se deben proteger estos dispositivos.

Los Smartphone son muy valiosos que ya en su interior tienen todos nuestros datos personales: fotos, contactos, videos, contraseñas, etc. Que para los ciberdelincuentes son muy atractivos todos estos datos, ya sea para lograr tener beneficios económicos como también para sólo causar daños.

Por ello es importante mantener precaución con lugares que son posiblemente sitios peligrosos, además también intentar antes de descargar alguna aplicación ver las puntuaciones que le dan los usuarios como los comentarios que aparecen de la aplicación.

El malware para Android seguirá aumentando significativamente a medida que más usuarios se interesen por este sistema operativo y mientras más vulnerabilidades encuentren los ciberdelincuentes, como se muestran en algunos tipos de malware antes eran inclusivos de ataques a PC pero ahora también se han propagado para los dispositivos móviles, aún no existen medidas que sean 100% exitosas sobre nuevo malware pero si existen estudios sobre poder detectar malware con técnicas que a futuro llegarán a ser asombrosas.

11. Referencias

1. http://www.iabspain.net/wp-content/uploads/downloads/2014/09/VI_Estudio_Anual_Mobile_Marketing_version_abierta1.pdf
2. http://www.av-comparatives.org/wp-content/uploads/2014/03/security_survey2014_es.pdf
3. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6320432
4. http://www.mcafee.com/us/resources/white-papers/wp-android-malware-past-present-future.pdf
5. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6603766
6. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6641036
7. http://jeuazarru.com/wp-content/uploads/2014/10/android_malware.pdf
8. http://www.welivesecurity.com/la-es/2014/08/01/cabir-a-simplocker-10-anos-malware-para-moviles/
9. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6481989
10. http://histinf.blogs.upv.es/files/2012/12/ANDROID-Gabriel-Herraiz-Ant%C3%B3n.pdf
11. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6675404
12. http://www.welivesecurity.com/wp-content/uploads/2014/02/tendencias_2013_vertiginoso_crecimiento_malware_moviles.pdf
13. http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf
14. http://blog.kaspersky.es/que-es-un-botnet/755/
15. http://www.pandasecurity.com/spain/mediacenter/consejos/que-es-un-ransomware/
16. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6888862

17. http://www.superame.com/estadisticas-del-uso-de-dispositivos-moviles-2013/